DIR CYBERSECURITY INSIGHT Newsletter

June 2014

ADDRESSING THE EVER CHANGING RISKS FOR THE STATE OF TEXAS

Score a goal in your Security Education.

Beginning September 2014 (FY 2015), the DIR Office of the CISO (OCISO) will begin a security education program for all State of Texas CISOs/ISOs.

The program will include a combination of technical security areas coming from the National Initiative for Cybersecurity Careers and Studies (NICCS) as well as Software Skills and Global certification training taught by Expanding Security. ISOs and CISOs will be able to fill in the blanks in much needed areas. Get ready to kick the ball and score a goal for your education and the State of Texas.

Stay tuned for more information to come.

If you can't explain simply, you don't understand it well enough.

- *Albert Einstein*

IN THIS ISSUE

Security 101 - Encryption

What to Encrypt

Texas Business & Commerce Code § 521.052

- A business shall implement and maintain **reasonable procedures**, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.
- A business shall destroy or arrange for the destruction of customer records containing sensitive personal information within the business's custody or control that are not to be retained by the business by:
  - Shredding;
  - Erasing; or
  - **Otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means**.

HIPAA / GLBA exceptions

- "Covered entities and business associates must only provide the required notifications if the breach involved **unsecured** protected health information. Unsecured protected health information is protected health information that has not been **rendered unusable, unreadable, or indecipherable** to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance." – HHS Security Rule Guidance

What Encryption Matters

- Financial data: credit card account numbers and tracking data, bank account numbers and associated financial information, credit-related data on individuals and businesses
- Personal health data: insurance-related data, actual medical information, and personal data about patients, such as Social Security numbers, addresses, and other sensitive information
- Private individual data: Social Security numbers, addresses and phone numbers, and other personally-identifiable data that could potentially be used for identity theft (see B&C 521)
- Confidential/sensitive business data: trade secrets, research and business intelligence data, management reports, customer information, sales data

Definitions

There are four parts to any crypto message:

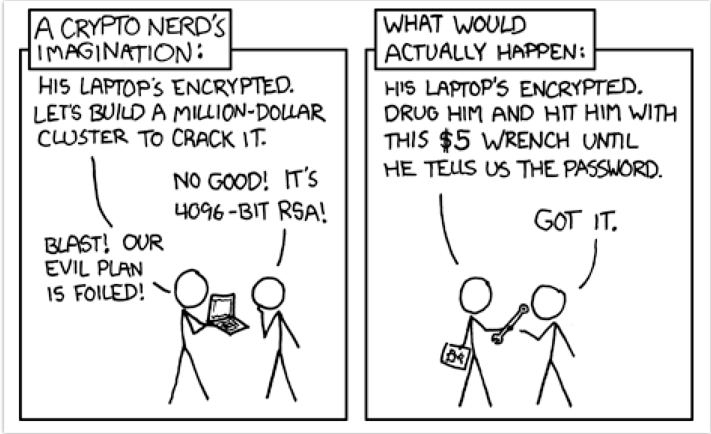
- Cleartext: the original, readable message
- Ciphertext: the scrambled, unreadable message
- Cipher: the method used to make cleartext "unreadable"
- Key: a piece of input that determines how the cipher outputs

Cryptography is a useful tool. It is **not** the solution to "security" as defined in the CIA triad.

A Slight Detour

Encryption	Hashing
• Reversible through decryption process • Allows for confidentiality • Will produce cypher text of variable size	• One-way, not "dehashable" • Supports integrity • Produces the same size output, regardless of input: ○ The word "Odyssey" = 5acdadef86e7173f2f90711b6b9d646b ○ *The odyssey* by Homer = 99c69a8c76f441af854aa43baff42da9 ○ *The Odyssey* by Homer (changing the case of the first letter) = dd93f7f85cf08943c78063503315bf62

So… redefine "brute force"


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

http://xkcd.com/538/

346d7afd6acc589815f4e2dfb5658d45:

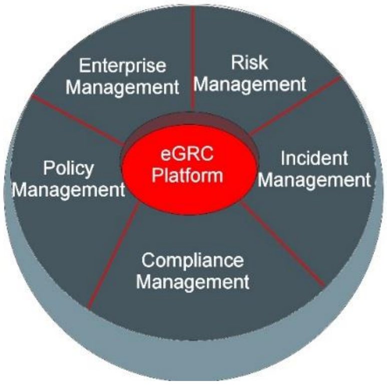
DIRSecurity@dir.texas.gov

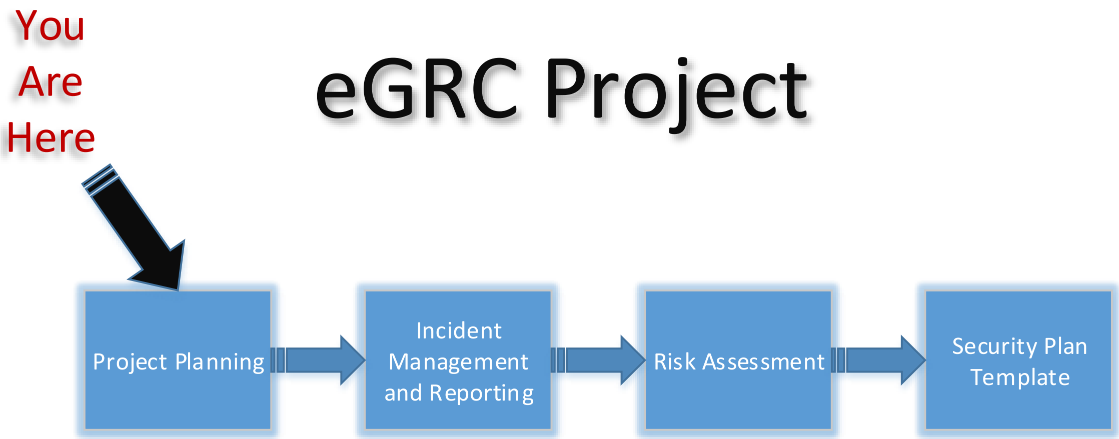
GRC - Governance, Risk, and Compliance

As mentioned in last month's Cybersecurity Insight, the OCISO is in the process of acquiring RSA Archer enterprise governance risk and compliance software for use by state agencies and institutions of higher education. Initial plans include:

1. Replace the Security Incident Response System (SIRS) and improve the security incident reporting process.
2. Replace the ISAAC Risk Assessment Tool.
3. Automate the creation of the Security Plan Framework Template.

Watch for further details in the upcoming Insight Newsletters as well as the monthly Information Security Working Group meetings.





Security Awareness for the 21st Century

SANS Securing the Human goes beyond compliance and focuses on changing human behavior through a variety of both training and testing tactics.

The OCISO has acquired 100,000 licenses for FY2015 with the objective of promoting awareness and enhancing agencies' security awareness programs.

If you would like to take full advantage of this service and implement a new and updated security awareness program for your employees, please contact us at: DIRSecurity@dir.texas.gov

JOE VOJE

I hold a Bachelor's Degree from Oregon State University (Go Beavs!) in History and a Master's Degree from Capitol College in Network Security. I started my career in the Navy as an enlisted Electronics Technician and eventually earned a commission as a Naval Officer. I retired from the Navy after 23 years of service. After the Navy, I consulted and worked in the financial and energy sectors. I joined the University of Texas – Pan American in 2012.

How did you come to the security field?

I think that like most security professionals, I arrived here completely by accident. But if I had to point to the most pivotal event that influenced my career in security, it was the cancelation of my military orders as a Communication Officer sending me to London, England, from Atsugi, Japan, and the subsequent reassignment to a position as the Information Assurance Officer for the US Pacific Fleet in Pearl Harbor, Hawaii. That is where I really became involved in information security on a national level and gained a lot of exposure to the trade.

Tell us how information security has changed since you started in your role.

The field drastically changed when we moved from a pure cyber warfare battlefield (destruction or theft of data) to a cyber-kinetic battlefield (code that could destroy something in the real world). Although Stuxnet is a few years old now, I don't think many executives understand the risk to our national infrastructure well enough to invest in the types of tools and trained personnel to prevent this type of threat from impacting us on a significant scale.

How did you first learn about The University of Texas – Pan American?

I was working as a consultant in Seattle, WA, and my mother was living in Deep South Texas. I wanted to be closer to her, so I started looking for work close to where she lived. I also wanted to work in higher education, so I conducted an Internet search for universities in the area. It must have been fate, because The University of Texas – Pan American had an opening for a CISO. I applied for the position and the rest is history.

What do you like best about your job?

The best part of my job is the opportunity to collaborate with intelligent people who are passionate about what they do for a living. Our faculty and staff members are completely dedicated to educating the next generation of leaders. And our students are eager to learn and apply themselves in their chosen fields of study.

Who are your users/customers, and what is one of the most challenging area for you?

Probably the biggest challenge is the diversity of applications and end user needs. Some customers only need an Internet connection and they are satisfied; others need bleeding edge technology. It creates a really unique environment to keep secure.

What other career would you have liked to pursue?

Billionaire. But I'd settle for a part-time gig in that field.

Tell us about your most proud accomplishment?

Earning my commission as a Naval Officer. It was a two-for-one deal. I was able to earn my bachelor's degree and advance my career in the Navy all on the same day.

What has been the greatest challenge that you have faced, and how did you resolved it?

Long separations from family during military deployments. You just keep yourself busy and avoid looking at calendars…eventually you find yourself pulling into port, the colors shift, and liberty call comes.

What is the best advice you have received and that you have used?

If you don't ask, the answer is always no.

What would be your advice for a new security professional?

Technical skills are required, but if you want to make it to the top, work on your people skills.

The University of Texas-Pan American (UTPA), a Hispanic serving institution, is in the middle of one of the fastest growing areas in the nation, the southern tip of Texas known as the Rio Grande Valley. UTPA is located in Edinburg, Texas.

Since its inception in 1927, UTPA has conferred over 2,600 associates, 61,000 bachelors, 13,000 masters, and 178 doctoral degrees.

Top 3 life highlights

1. Birth of my two great kids.
2. Serving my country for over 20 years around the globe. Too many adventures to list.
3. Visiting my ancestral home in Norway.

And where did you grow up?

I grew up in the Pacific Northwest.

Do you have family in Austin?

No family in Austin. Most of my family lives either in the Pacific Northwest or Deep South Texas.

What are your hobbies?

I enjoy riding my motorcycle and sailing…neither of which I do nearly enough. I'm usually preoccupied with DIY projects around my house.

People would be surprised to know that you…

1. Have spent time above the Arctic Circle.
2. Slept on the bow of a ship overnight from Greece to Italy.
3. Had to hire an interpreter in Istanbul, Turkey, to negotiate a "traffic incident."

Any favorite line from a movie?

"Gentlemen, you can't fight in here! This is the War Room!" From Dr. Strangelove or: How I Learned to Stop Worrying and Love the Bomb.

Are you messy or organized?

Chaos is a sign of intelligence…or at least that is what I tell myself to justify the state of my desk.

Favorite travel spot?

Italy.

What books are at your bedside? Or which one was the last one you read?

I keep a Kindle at my bedside, so I have a lot of books available. The last book I read was Red Rising, a modern dystopia about a futuristic cast system. A good read.

What is the CD that you have in your car?

During my five-minute commute from home to work, I usually listen to Jack FM or some personal Pandora Station.

If you could interview one person (dead or alive) who would it be?

I know he's not a person, but I'd really like to know what my dog is thinking. He's a Golden Retriever, so he's always smiling…He's got to be the happiest "person" I know.

If you had to eat one meal, every day for the rest

Pasta in any of its many forms and preparations.

Least favorite Food?

Serving in the Navy you learn to eat anything. It all tastes the same with enough hot sauce on it.

If given a chance, who would you like to be for a day?

I'm pretty comfortable in my own skin, but I suppose I'd like to be, Manfred von Richthofen, a.k.a., "The Red Baron" for a day. Just not the day he finally got shot down for good.

If you were to write a book about yourself, what would you name it?

The real trick would be getting it published.

Describe what you were like at age 10

Too tall, too skinny. I miss that kid.

Collaboration Opportunities

Statewide Information Security Advisory Committee

The Statewide Information Security Advisory Committee (SISAC) provides guidance to the Texas Department of Information Resources (DIR) on the Statewide Information Security Program. The committee, chartered by DIR in 2011, is comprised of information security professionals from state and local government and representatives from private industry.

Join a Team

Contribute to SISAC by participating in one of its subcommittees. These workgroups meet on a monthly basis.

- **Communications Subcommittee**
  Communicates to the agencies the progress of the DIR Statewide Information Security Program and associated events and evaluates feedback from the agencies. To join, contact Frosty Walker, ISO, Texas Education Agency (Frosty.Walker@tea.state.tx.us).

- **Privacy Subcommittee**
  Facilitates collaboration with agency personnel responsible for privacy policy functions associated with the protection of citizen privacy and developing privacy incident response procedures. To join, contact Elizabeth Rogers, CPO, Texas Comptroller of Public Accounts (Elizabeth.Rogers@cpa.state.tx.us).

- **Solutions Subcommittee**
  Evaluates solutions to common problems and shares best practices among agencies. To join, contact Claudia Escobar, Statewide Security Services Delivery Lead. Department of Information Resources (Claudia.Escobar@dir.texas.gov).

- **Risk Assessment Subcommittee**
  Defines and maintains the state's risk assessment methodology. To join, contact Shirley Erp, CISO, Health and Human Services Commission (Shirley.Erp@hhsc.state.tx.us).

- **Policy Subcommittee – (membership currently closed)**
  Defines the state's security policy through the development of rules, standards, policies, and guidelines. For information, contact Edward Block, Deputy CISO, Department of Information Resources (Edward.Block@dir.texas.gov).

- **Security Workforce Development**
  Studies security workforce issues and advises SISAC on recommendations to enhance the state's security workforce. To join, contact Jesse Rivera, CISO, Texas Comptroller of Public Accounts (Jesse.Rivera@cpa.state.tx.us).

A New Solutions Subcommittee

You are the piece missing in this puzzle! Participate and provide value for your agency and for the State of Texas.

A new collaboration Solutions Subcommittee has emerged as a response to the ever changing environment that the security professional faces every day. Duties for this team will be:

- To promote technology leadership and opportunities for enterprise collaboration within cybersecurity
- Evaluate solutions for issues identified through the various assessment activities performed throughout the state
- Assess vendor service and product solutions provided through the Framework's Vendor Alignment Template
- Provide support to the Information Security Officer Roundtable Group

Please join us on July 9th at 9:00 am at the DIR offices, or join us remotely. More information will be sent soon.

Brian Engle CISO

Insight from our Texas CISO

Senate Bill 1597 Testimony

On June 18th, I testified before the Senate Committee on Government Organization to provide information on cybersecurity and specifically provide an update on the implementation progress of Senate Bill 1597 related to Agency Security Plans. The written and oral testimony provided details for the timeline of events and activities related to the creation of the Agency Security Plan Template as well as what we learned from the survey conducted by the Statewide Information Security Advisory Committee (SISAC) Communications Subcommittee. Additionally, the testimony included emphasis on several key points related to cybersecurity within the state.

The first point that I shared is that protection is important but not all there is to a security program. As the Agency Security Plan Template reinforces, the importance of a complete security program includes not only protection of information and information resources, but also that considers that it is critical to have effective detection, response, and recovery processes. Protection cannot equate to 100% prevention of security events, and the ability to detect and respond when events occur is essential.

Second, I advised the committee members that often when programs mature and capabilities increase, the ability to detect issues also increases. When this happens, it seems as if things have gotten worse rather than better, which can be contrary to expected outcomes. Improvements that we will make in the areas of incident management and reporting along with the implementation of improvements related to program maturity that should occur with the implementation of the Agency Security Plan processes may reveal more accurate risk levels. As we implement the Governance, Risk, and Compliance platform and replace the Security Incident Reporting System (SIRS) in the upcoming months, the visibility of risk will improve. The increase in visibility may reveal more issues than we can currently see.

Lastly, I described the landscape that we are confronted with when asked if the state is secure. Tomorrow is promised to no one, but many constants remain. Technology risk continues to increase at every stage of change and innovation. The pace is quick and increasing, and the requirements for protecting information and information systems are not growing easier. Complexity, human behaviors, and the ever increasing demands for technology solutions all place strains on processes that we require to operate securely in our organizations. People are an important part of the equation, a significant reason that the job of information security belongs to everyone, and also a reason why the job is never done.

I hope you find the DIR Cybersecurity Insights useful, and I look forward to sharing my insights with you in future issues.

Brian Engle
State of Texas CISO

Around the Corner

Cybersecurity Incident Briefing

What: Verizon/Cyber Trust's 2014 Data Breach Investigative Report
Cost: Free
When: Tuesday, July 8th, 1:30 – 3:30 pm, Travis Bldg., Room 1–100
Info: DIRSecurity@dir.texas.gov

Monthly Security Program Webinar

What: July's webinar "Is Your IAM Environment Ready for Office 365"
Cost: Free
When: Tuesday, July 15th, 2:00 – 3:00 pm CDT
Info: https://www1.gotomeeting.com/register/904973177

Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas